

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

MATTHEW HASH,

Defendant.

)
)
)
)
)
)
)

UNDER SEAL

CASE NO. 1:19-MJ-119

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, Ryan Saraceni, being duly sworn, hereby depose and state as follows:

Introduction

1. I, Ryan Saraceni, am a Special Agent employed by the United States Secret Service ("USSS") and have been so employed for over two years. As a Special Agent of the USSS, I received training in investigating violations of federal statutes, including those regarding conspiracy, wire fraud, money laundering, and the manufacture and possession of counterfeit U.S. currency. I have participated in numerous counterfeit U.S. currency, criminal enterprise, and financial investigations. More specifically, I have conducted physical surveillance, executed arrest and search warrants, analyzed phone and text records, and obtained and reviewed financial documents and records of fraudulent activity. I have also spoken to suspects, defendants, witnesses, and other experienced investigators concerning the methods and practices of criminal enterprise groups, especially those involved in wire fraud and aggravated identity fraud. For seven months, I have investigated a variety of white-collar crime cases, including bank fraud, check fraud, wire fraud, aggravated identity theft, and counterfeit U.S. currency.

2. This affidavit is made in support of a criminal complaint and arrest warrant charging Matthew Hash with conspiracy to commit wire fraud, in violation of Title 18, United States Code, Sections 1343 and 1349.

3. This affidavit is based on my personal investigation and the investigation of others, including federal and local law enforcement officials whom I know to be reliable, and agents and employees of TJX Companies, Inc. The facts and information contained in this affidavit are based upon information provided by those individuals, witness and suspect interviews, and my review of records, documents, and other physical evidence obtained during this investigation.

4. This affidavit does not include each and every fact known to the government, but only those facts necessary to support a finding of probable cause to support the requested arrest warrant.

Probable Cause

5. As explained below, the Montgomery County Police Department ("MCPD") and the USSS have conducted an investigation into the unauthorized use of account numbers for gift cards issued by stores operated by TJX Companies, Inc. ("TJX"), which include T.J. Maxx, Marshalls, and Home Goods. TJX stores specialize in the sale of consumer apparel, jewelry, and home goods. The joint investigation uncovered a conspiracy among various individuals, including Hash, to procure existing account numbers for TJX gift cards that belonged to other individuals and to use them, without authorization, to purchase items from TJX stores in various states, including within the Eastern District of Virginia. The unauthorized use of the gift cards was effectuated in part through the use of interstate wire transmissions.

A. Overview of TJX Gift Card Process

6. Each gift card that TJX issues has a unique account number. That number is printed on the gift card itself and is also encoded electronically onto the card. The encoded number comes up when a card with an electronic strip is scanned at a point of sale. It is the number that is charged upon a sale.

7. On legitimate TJX gift cards, the physical and electronic numbers match. TJX maintains records of its gift cards—including the number and dollar amounts associated with them—on an internal electronic database known as a Stored Value Card (SVC) portal. Salaried employees in TJX's Loss Prevention group have access to a program called ASPECT, which also contains gift card account information.

8. "Cloning" is a process used to create illegitimate and fraudulent gift cards. It involves re-encoding a gift card with an account number that does not match the physical number printed on the card and that is usually stolen. Unlike a legitimate gift card, when a "cloned" card is scanned at a point of sale, an account number other than the account number displayed on the physical card is charged.

9. During the times relevant to the events described below, TJX contracted with a Florida-based company, Smartclixx, to process its financial transactions that involve TJX gift cards. During retail transactions at TJX stores, sales and returns data were transmitted immediately by wire from the cash register terminals at the point of sale to Smartclixx in Florida. Backup data from the transactions were then sent to the TJX mainframe computer in Ohio. The SVC portal accessed Smartclixx information via wire communication for review and analysis.

B. Investigation

10. In or around 2014, TJX launched an internal investigation after it noticed an uptick in customer complaints related to gift cards that were issued with a certain monetary value but that, upon use, no longer had the same value or had no value remaining at all, even though the customer had not used the monetary credit on those gift cards.

11. TJX's Loss Prevention Group investigated the complaints of fraudulent gift card use. Its internal investigation revealed that the general scheme involved subjects who used cloned gift cards to purchase items at TJX stores, including Marshalls, T.J. Maxx, and Home Goods. TJX discovered that many of the cloned gift cards had been re-encoded with account numbers from high-value dollar cards, most of which had been issued to customers in the Northeast region of the United States. Subjects later returned the merchandise that had been purchased with a cloned gift card for a store credit in the form of a new—now “clean”—TJX gift card. The account numbers printed on the new “clean” TJX gift cards matched the number electronically encoded onto them.

12. The investigation revealed that an employee of TJX (hereafter “CC-1”) was involved in the scheme. CC-1 was employed as an Internal Fraud Investigator by TJX. His primary duties included investigating internal fraud in Northern Virginia and West Virginia. As part of his job, CC-1 had access to TJX's SVC portal and ASPECT. CC-1 was therefore able to identify high-value gift cards and their associated account numbers using ASPECT. In fact, CC-1 logged on to ASPECT and obtained information about high-value gift cards, including account numbers.

13. CC-1 has since been criminally prosecuted and convicted for his involvement in this unlawful scheme. CC-1 pleaded guilty to conspiracy to commit wire fraud, in violation of

18 U.S.C. § 1349. Pursuant to his plea agreement, CC-1 agreed to cooperate with the government. Accordingly, CC-1 has provided the government with information regarding Hash's participation in the conspiracy. I believe CC-1 to be reliable because information he provided was corroborated by other evidence.

C. Origination of Conspiracy

14. In connection with his guilty plea, CC-1 admitted that, "[d]uring the course and in furtherance of the conspiracy, [he] provided the account numbers of approximately 140 TJX gift card accountholders, without their authorization, to unindicted co-conspirators which were then 'cloned' and used to obtain retail goods and/or 'clean' gift cards, resulting in a loss of approximately \$201,718.22 to TJX."

15. CC-1 has informed the government that he originally worked with another co-conspirator ("CC-2") in the fraudulent scheme. According to CC-1, he would identify the account numbers of high value TJX gift cards using ASPECT. CC-1 would then use a reader/writer to encode, or "clone," those gift card account numbers onto blank gift cards at CC-2's home. CC-1 stated that CC-2 and CC-2's team would then use those cloned gift cards to make purchases and get refunds in the form of new, "clean" gift cards. According to CC-1, CC-2 would then sell the clean gift cards to Hash.

16. In connection with his guilty plea, CC-1 admitted that he first met Hash in or around December 2014. CC-1 has informed the government that CC-2 introduced him to Hash at the "Oxford House" in Rockville, Maryland. The Oxford House was Hash's residence at the time.

17. According to CC-1, when he first met Hash at the Oxford House, Hash laid out a plan to recruit a team to make purchases and returns with fraudulent TJX gift cards and to obtain

genuine TJX gift cards. As part of Hash's plan, Hash's company, "Capital Gift Cards," would then sell those genuine TJX gift cards to another gift card purchasing company. No agreement was reached during this initial meeting, however.

18. CC-1 stated that when he got home from the meeting with Hash, he received a shut-off notice from his utility company. At that point, CC-1 called Hash and informed him that he was willing to provide Hash with encoded gift cards. According to CC-1, he and Hash agreed to split the proceeds of the scheme 50/50. CC-1 provided the TJX gift card information, which he encoded onto blank cards using his reader/writer at Hash's room in the Oxford House. Hash provided the blank cards and recruited the team to make purchases and returns at TJX stores. According to CC-1, Hash paid CC-1 mainly in cash. Hash and CC-1, moreover, agreed to cut CC-2 out of the scheme. Hash later told CC-1 that CC-2 had been ripping CC-1 off.

19. After reaching this agreement with CC-1, Hash and other unindicted co-conspirators then used the re-encoded, or "cloned," gift cards to purchase merchandise at TJX stores in the Eastern District of Virginia and elsewhere. They would then return the merchandise at TJX stores for new, "clean" gift cards.

D. Hash's Use of Cloned Gift Cards

20. As the below examples illustrate, surveillance images reflect Hash conducting a number of these fraudulent transactions at TJX stores. For each transaction described in paragraphs 21 to 25, surveillance images were obtained from TJX. MCPD officers then compared the images with Maryland Motor Vehicle Administration ("MVA") photographs of Hash. Through that comparison, they identified Hash as the subject conducting the transactions.

21. On or about January 4, 2015, Hash entered a Marshalls store (store 209) located in Rockville, Maryland. There, Hash purchased three pairs of high-end designer shoes for \$922.17

using multiple TJX gift cards, including a gift card with the account number ending in -8430. The transaction caused a wire transmission between Smartclixx in Florida and TJX's SVC system in Ohio. Hash then left the store with the merchandise. The gift card account number ending in -8430 was generated in Kingston, New York, on September 11, 2014. The card owner's assistant later confirmed that the card was compromised and that the card owner had not been to Maryland to make any purchases. TJX reimbursed the card owner for the unauthorized purchases and suffered a loss as a result.

22. On or about January 24, 2015, Hash entered a Marshalls store (store 548) located in Sterling, Virginia, within the Eastern District of Virginia. There, Hash made two purchases, causing a wire transmission between Smartclixx in Florida and TJX's SVC system based in Ohio. Hash purchased one pair of shoes, two new, "clean" \$100.00 gift cards, and two new, "clean" \$125.00 gift cards. Hash used a TJX gift card with the account number ending in -2964 to purchase the items for \$491.34. Hash then left the store with the gift card and the merchandise. Subsequently, on February 3, 2015, TJX received a customer complaint regarding missing funds on the gift card with the account number ending in -2964. The customer stated that the purchases made on January 24, 2015, in Sterling, Virginia, were not authorized. TJX subsequently reimbursed the customer in the amount of \$491.34, suffering a loss as a result.

23. On or about March 6, 2015, Hash entered a Marshalls store (store 482) located in Philadelphia, Pennsylvania. Hash purchased two men's items for \$22.99 and one new, "clean" \$250.00 gift card. Hash paid for the items using a gift card with the account number ending in -4299. Hash also purchased a second new, "clean" \$250.00 gift card, which he paid for using the same gift card with the account number ending in -4299. The purchases caused a wire transmission between Smartclixx in Florida and TJX's SVC system in Ohio. The card ending in

-4299 was generated in Bridge Water, New Jersey, on February 20, 2015. TJX subsequently received a complaint from the customer to whom the gift card ending in -4299 was issued. The customer claimed not to have authorized the purchases made on March 6, 2015, in Philadelphia. TJX reimbursed the customer's gift card balance for these transactions and suffered a loss as a result.

24. On or about March 19, 2015, Hash entered a T.J. Maxx store (store 851) located in Sterling, Virginia, where he made two purchases for gourmet food and fragrance, which caused a wire transaction between Smartclixx in Florida and TJX's SVC system in Ohio. The first transaction totaled \$37.01, which Hash paid for using a gift card with the account number ending in -6881. The second transaction was for \$5.11, which Hash paid for using a gift card with the account number ending in -3940. The card ending in -6881 was generated in Los Angeles, California, on February 24, 2015. The card ending in -3940 was generated in Feasterville, Pennsylvania, on February 16, 2015. Hash then left the store with the merchandise.

25. The next day, on March 20, 2015, as a result of multiple reports of the use of fraudulent gift cards, TJX investigators conducted surveillance at a T.J. Maxx store (store 277) located in Olney, Maryland. Investigators observed a suspect believed to be a co-conspirator of Hash ("CC-3") enter the store. TJX investigators previously knew of CC-3 because he had conducted non-receipted returns of store merchandise purchased with cloned gift cards, at which time CC-3 had to provide photographic identification. While in store 277 on March 20, CC-3 made a purchase, causing a wire transmission between Smartclixx in Florida and TJX's SVC system in Ohio. CC-3 purchased one piece of jewelry totaling \$534.24 and paid with a gift card with the account number ending -6881—the same gift card account number that Hash had used

for a small purchase the day before, as described in paragraph 24. CC-3 left the store with the jewelry.

26. TJX investigators observed CC-3 get into a Toyota Corolla with Maryland license plate 3ELW02. Local law enforcement had previously seen the same Toyota Corolla at Hash's residence at the Oxford House. Moreover, a query of the Maryland MVA database revealed the vehicle was registered to an individual who, according to a public source database and other law enforcement records, is the father of Matthew Hash. Later on March 20, 2015, TJX employees went to the Oxford House, where Hash resided, and observed the same Toyota Corolla parked there.

E. Search of Hash's Residence

27. On April 30, 2015, the MCPD executed a state search warrant at Hash's residence at the Oxford House in Rockville, Maryland. The MCPD seized, among other things, a credit card encoder, multiple gift cards, and an Apple iPhone with the phone number (240) 477-0669.

28. During the search, the MCPD officers also found and seized numerous TJX gift cards from Hash's residence. TJX investigators identified that approximately 77 of the seized TJX gift cards were re-encoded or cloned with unauthorized gift card account numbers that did not match the gift card account number printed on the gift cards. In addition, the officers found receipts that matched purchases that Hash and CC-3 made with fraudulent, "cloned" TJX gift cards as well as "clean" TJX gift cards. They also found documents that appeared to be invoices and order forms to and from Hash and a company called "Card Cash" in New Jersey for the sale of gift cards.

F. Communications Between Hash and CC-1

29. Pursuant to the April 30, 2015 search and seizure warrant at Hash's former residence, which included electronics and contents therein, law enforcement searched the contents of Hash's cell phone related to phone number (240) 477-0669. The contents of the phone reflect that Hash used it. It contained multiple photos and videos of Hash, numerous links to social media site accounts held by Hash, text messages, emails, and phone contacts.

30. Hash's cell phone contained a contact described in the phone as "Superfly (Gift Card)." The phone number for "Superfly (Gift Card)" was (703) 855-4031. Records obtained from Sprint reflect that the number (703) 855-4031 belonged to CC-1. CC-1 also listed that number as a contact number for himself on TJX personnel forms.

31. AT&T records for Hash's cell phone number reflect 45 phone calls between Hash and CC-1 from December 3, 2014, and April 4, 2015.

32. According to Sprint records, CC-1's cell phone was in regular contact with Hash between May 1, 2015, and June 9, 2015, that is, even after the execution of the state search warrant.

33. Hash's cell phone contained text messages that he exchanged with CC-1 at "Superfly (Gift Card)." Based on my training and experience, and the facts uncovered in this investigation, I understand Hash and CC-1 to have used coded language to discuss their scheme and efforts to avoid detection. These text messages included, but are not limited to, the following:

- a. On December 16, 2014, Hash's cell phone sent the following message to CC-1 at "Superfly (Gift Card)":

Yeah sent him in with 4 coupons all labeled & numbered.
He said there was little on most of them and that

the combined total was \$400 or so. He said the clerk combined all the cards onto one card and then cut all the cards in half. I completely flipped on him but he's adamant that nobody suspected anything and that he's telling me the truth. I just got to make sure because on top it all, this is the very first time I've given him coupons without already knowing the amount on them. The deck today has been on point so for him to come out with this story and no receipts is just hard to swallow.

Based on the facts uncovered in the investigation, I understand that the term "coupons" refers to the gift cards and that the term "numbering" means the amount contained on the gift card was written on the card.

- b. Earlier in the day on December 16, CC-1 sent a message to Hash's cell phone, stating as follows: "Word is, images are being collected form [sic] Maryland area. Trying to identify the members of the book club." Based on the facts uncovered in the investigation, I understand that "members of the book club" is a reference to Hash and his associates who were conducting the activity in the stores. Thus, based on the facts uncovered in the investigation and my training and experience, I understand CC-1 to have been warning Hash about TJX's investigation
- c. On January 13, 2015, Hash sent a message to CC-1 stating, "If it's possible let's try to do 2x the norm.. I've got plenty of blank canvas. So were good.." Based on the facts uncovered in the investigation, I understand that "blank canvas" refers to the gift cards that are yet to be re-encoded.
- d. On January 14, 2015, Hash sent a message to CC-1 stating, "We might have an issue the first 3 cards came up invalid b 4 one worked!! Like they were written wrong maybe." Based on the facts uncovered in the investigation, I understand

that “written wrong” means that the cards were not re-encoded correctly, which led to them not being able to be read at the point of sale terminal. Thus, based on the facts uncovered in the investigation and my training and experience, I understand the issue described in the text means that the cards were not readable.

- e. On February 17, 2015, Hash sent the following message to CC-1: “Looks like I’m not even gonna make it outta town. How hot is NOVA right now?” Northern Virginia can be abbreviated as NOVA. “Hot” is a common term used by criminals to describe law enforcement presence. CC-1 responded: “I have not heard anything about them watching that area. That’s not even a BOLO as far as I have heard.” The term “BOLO” is an acronym used by police and loss prevention that means “be on the lookout.”
- f. On April 30, 2015, Hash sent the following message to CC-1: “I owe you another \$398 that should bring the total to \$4558.”

34. CC-1 and Hash continued to communicate with each other even after the search warrant was executed at Hash’s residence on April 30, 2015. According to CC-1, Hash did not immediately tell him about the search warrant conducted on Hash’s residence.

35. TJX store surveillance video revealed that between June 20, 2015, and June 23, 2015, Hash and his co-conspirators used cloned or duplicate gift cards in at least thirty different TJX-owned stores in New Jersey, Pennsylvania, and Delaware. According to TJX, the loss amount for the fraudulent transactions over this three-day period alone was over \$12,000.

G. Search Warrants on Hash’s New Residence and CC-1’s Residence

36. On September 2, 2015, the USSS and MCPD executed a federal search warrant at Hash’s new residence in Bethesda, Maryland. Hash was found in the rear bedroom pushing

items into a hole in the wall. Items seized during the search warrant included, but were not limited to, a fake identification card with the name "Richard Davis Moneymaker" from Washington, D.C., with Hash's photograph on it, and 150 TJX gift cards. Investigators identified 36 of the TJX gift cards as cloned because, when they scanned each of the cards, the encoded number did not match the embossed number on the card.

37. The same day, on September 2, 2015, USSS and Prince William County Police executed a federal search warrant for CC-1's residence at Dale Boulevard in Dale City, Virginia. CC-1 was in the basement bedroom and was asked to come to the front door area. Numerous documents and items were recovered from the residence, including phones, several laptop computers, tablets, computer disks, flash drives consisting of mini flash cards and compact cards, and thumb drives.

38. On October 9, 2015, a federal search warrant was obtained to conduct a forensic analysis of the electronic evidence seized from CC-1's residence. The USSS Electronic Crimes Task Force imaged the items. An analysis of one of the thumb drives seized from CC-1's residence revealed a list of 55 gift card account numbers, some of which were the same account numbers on cards used by Hash and CC-3.

39. A review of the order forms and invoices seized from Hash's residence on April 30, 2015, reveals that Hash sold 33 "clean" TJX gift card account numbers to "Card Cash." As reflected in TJX records, these "clean" gift card account numbers were purchased by Hash and CC-3 on March 14, 2015, and March 15, 2015, from stolen TJX gift card account numbers found on CC-1's thumb drive.

Conclusion


40. Based on my training and experience, and the information provided in this affidavit, I respectfully submit that there is probable cause to believe that beginning on a date unknown, but from at least on or about December 2014 to September 2, 2015, within the Eastern District of Virginia, Matthew Hash and others committed conspiracy to commit wire fraud, in violation of Title 18, United States Code, Sections 1343 and 1349.

I declare under penalty of perjury that the statements above are true and correct to the best of my knowledge and belief.



Special Agent Ryan Saraceni
United States Secret Service

Sworn to and subscribed before me
this 8 day of March



The Honorable Theresa Carroll Buchanan
United States Magistrate Judge